035-0066

# 日　本　国　特　許　庁
# JAPAN　PATENT　OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:　２００２年１０月１０日

出願番号
Application Number:　特願２００２－２９７５５０

[ST.10/C]:　[ＪＰ２００２－２９７５５０]

出願人
Applicant(s):　株式会社東芝

２００３年　１月２４日

特許庁長官
Commissioner,
Japan Patent Office　太田信一郎

出証番号　出証特２００３－３００１３２４

【書類名】　特許願

【整理番号】　A000203876

【提出日】　平成14年10月10日

【あて先】　特許庁長官　殿

【国際特許分類】　H04L 12/00

G06F 12/00

【発明の名称】　ネットワークシステム、情報処理装置、中継器およびネットワークシステムの構築方法

【請求項の数】　16

【発明者】

【住所又は居所】　東京都青梅市末広町２丁目９番地　株式会社東芝青梅事業所内

【氏名】　武田　淳

【特許出願人】

【識別番号】　000003078

【氏名又は名称】　株式会社　東芝

【代理人】

【識別番号】　100058479

【弁理士】

【氏名又は名称】　鈴江　武彦

【電話番号】　03-3502-3181

【選任した代理人】

【識別番号】　100084618

【弁理士】

【氏名又は名称】　村松　貞男

【選任した代理人】

【識別番号】　100068814

【弁理士】

【氏名又は名称】　坪井　淳

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100070437

【弁理士】

【氏名又は名称】　河井　将次

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　　ネットワークシステム、情報処理装置、中継器およびネットワークシステムの構築方法

【特許請求の範囲】

【請求項１】　ネットワーク接続を行う端末と、

前記端末の接続要求に際して認証を行うサーバと、

前記端末からの認証要求を受け付け、当該要求受付時の情報をもとに前記端末の認証を行うサーバを特定し、前記要求を行った端末を前記特定したサーバに接続する処理装置と

を具備したことを特徴とするネットワークシステム。

【請求項２】　前記端末の認証を行うサーバは、ドメイン若しくはそれに類するネットワーク環境毎に設けられ、前記端末は、ドメイン若しくはそれに類するネットワーク環境に特定されることなく設けられる請求項１記載のネットワークシステム。

【請求項３】　前記処理装置は、前記端末から前記要求を受け付けたとき、当該要求受付時の情報をもとに要求元の端末が所属するドメイン若しくはそれに類するネットワーク環境を認識し、自己の所属するドメイン若しくはそれに類するネットワーク環境に所属するとき、前記サーバを特定する処理および前記接続の処理を実行する請求項１記載のネットワークシステム。

【請求項４】　前記処理装置と前記端末は、無線ＬＡＮにより接続される請求項１記載のネットワークシステム。

【請求項５】　ネットワーク接続を行う端末装置から認証要求を受け付ける手段と、

前記受け付けた要求をもとに当該要求を行った端末装置のアクセス資格の有無を検証する装置を特定する手段と、

前記要求を行った端末装置を前記特定した装置に接続する手段と

を具備したことを特徴とする情報処理装置。

【請求項６】　前記要求を行った端末装置のアクセス資格の有無を検証する装置を特定する手段は、前記要求受付時の情報をもとに前記端末装置の識別名を

取得し、当該識別名を用いたマッチングにより、前記端末装置が所属するドメイン若しくはそれに類するネットワーク環境を認識し、その認識結果をもとに前記要求を行った端末装置のアクセス資格の有無を検証する装置を特定することを特徴とする請求項５記載の情報処理装置。

【請求項７】　端末の接続要求に際して認証を行うサーバを具備したネットワークシステムに設けられる中継器であって、

端末からの認証要求をもとに当該要求を行った端末の認証を行うサーバを特定する手段と、

前記要求を行った端末を前記特定したサーバに接続する手段と

を具備したことを特徴とする中継器。

【請求項８】　前記サーバを特定する手段は、ネットワーク接続可能な複数のドメイン若しくはそれに類するネットワーク環境と、その各ドメイン若しくはそれに類するネットワーク環境に置かれた認証を行うサーバとを対応付けて管理するテーブルを有し、前記要求の受付時に、前記端末より取得した情報と前記テーブルとを用いて、前記要求を行った端末の認証を行うサーバを特定することを特徴とする請求項７記載の中継器。

【請求項９】　前記端末との間で、ＩＥＥＥ　８０２．１Ｘの定義に従い、前記認証の手続きを行うことを特徴とする請求項７記載の中継器。

【請求項１０】　前記端末との間で、ＥＡＰによる認証プロトコルを用いて前記認証の手続きを行うことを特徴とする請求項７記載の中継器。

【請求項１１】　ネットワーク接続に際して認証を必要とするサプリカントと、

前記サプリカントの認証要求に際して認証を行うオーセンティケーションサーバと、

前記サプリカントから前記要求を受け付けて当該端末の認証を行うオーセンティケーションサーバを特定し、前記要求を行ったサプリカントを前記特定したオーセンティケーションサーバに接続するオーセンティケータと

を具備したことを特徴とするネットワークシステム。

【請求項１２】　前記オーセンティケータは、ネットワーク接続可能な複数

のドメイン若しくはそれに類するネットワーク環境に置かれたオーセンティケーションサーバ各々をその所属するドメイン若しくはそれに類するネットワーク環境とともに管理するテーブルを有して、前記サプリカントからの前記要求受付時に、当該サプリカントの識別情報を取得し、前記テーブルに設定されているドメイン若しくはそれに類するネットワーク環境の情報と前記取得した識別情報とのパターンマッチングにより前記端末の認証を行うオーセンティケーションサーバを特定する請求項１１記載のネットワークシステム。

【請求項１３】　前記オーセンティケータは、ＩＥＥＥ　８０２．１Ｘの定義に従い、前記サプリカントとの間で前記認証の手続きを行うことを特徴とする請求項１１記載のネットワークシステム。

【請求項１４】　前記オーセンティケータは、ＥＡＰによる認証プロトコルを用いて前記サプリカントとの間で前記認証の手続きを行うことを特徴とする請求項１１記載のネットワークシステム。

【請求項１５】　ネットワーク接続を行う端末と、前記端末からの要求に従い前記端末をネットワークに接続する中継装置と、前記端末の接続要求に際して認証を行うサーバとを具備したネットワークシステムの構築方法に於いて、

前記中継装置に、

前記端末からの認証要求を受け付け、当該要求受付時の情報をもとに前記端末の認証を行うサーバを特定する手段と、

前記要求を行った端末を前記特定したサーバに接続する手段とを備えて、

前記端末が自己の認証を行うサーバとは異なるネットワーク環境下に於いても自己の認証を行うサーバとの間で認証手続きを行うことができるようにしたことを特徴とするネットワークシステムの構築方法。

【請求項１６】　前記端末の認証を行うサーバを特定する手段は、ネットワーク接続可能な複数のドメイン若しくはそれに類するネットワーク環境と、その各ドメイン若しくはそれに類するネットワーク環境に置かれた認証を行うサーバとを対応付けて管理するテーブルを有し、前記要求の受付時に、前記端末より取得した情報と前記テーブルとを用いて、前記要求を行った端末の認証を行うサーバを特定することを特徴とする請求項１５記載のネットワークシステムの構築方

法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、高度の認証手続きを必要とするネットワーク環境に適用される、ネットワークシステム、情報処理装置、中継器およびネットワークシステムの構築方法に関する。

【０００２】

【従来の技術】

ネットワークへのアクセスに際して十分なセキュリティを確保する際、ユーザ認証のための装置が用いられる。代表的なユーザ認証装置として、ＲＡＤＩＵＳサーバが知られている（非特許文献１参照）。

【０００３】

ＩＥＥＥ　８０２．１Ｘは、ポート単位でアクセスを制御するための規格である（非特許文献２参照）。具体的には、ネットワークに参加しようとする機器（ポートに接続した機器）に対して、認証処理をおこなう。そして、認証に成功した機器だけをネットワークに参加（ポートを開く）させる。

【０００４】

ここで言うポートとは、イーサネットＬＡＮケーブルのような物理的なポートだけではなく、論理的なものも含まれる。たとえば、無線ＬＡＮネットワークの場合、ステーション（ＳＴＡ）とアクセスポイント（ＡＰ）間の接続が確立したとき（アソシエーションが確立したとき）、ステーション（ＳＴＡ）がポートに接続したとみなすことができる（図１に示すＳＴＡ、ＡＰ参照）。

【０００５】

ＩＥＥＥ　８０２．１Ｘでは、以下の３つの構成単位（コンポーネント）が定義されている。

【０００６】

（１）．サプリカント（Ｓｕｐｐｌｉｃａｎｔ）

；認証されるコンポーネント。

【０００７】

（２）．オーセンティケータ（Ａｕｔｈｅｎｔｉｃａｔｏｒ）

；サプリカント（Ｓｕｐｐｌｉｃａｎｔ）のアクセスを制御するコンポーネント。ポートの開閉をおこなう。

【０００８】

（３）．オーセンティケーションサーバ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｓｅｒｖｅｒ）

；サプリカント（Ｓｕｐｐｌｉｃａｎｔ）の認証を行うコンポーネント。

【０００９】

しかしながら、ＩＥＥＥ　８０２．１Ｘでは、特にオーセンティケータから、オーセンティケーションサーバへの通信について細かい規定がない。したがって、従来の技術に於いては、オーセンティケータは、あらかじめ指定していた（複数の）オーセンティケーションサーバに対して、固定的に通信を行っていた。これは、オーセンティケーションサーバが、すべてのサプリカントの認証を請け負うことを前提としている。

【００１０】

この従来の技術では、互いに独立している環境下のサプリカントを、互いのネットワークに参加できるように再設定したい場合に、非常にコストがかかることがある。

【００１１】

たとえば、図７に示すように、オーセンティケーションサーバを各々にもつドメインＡとドメインＢのネットワーク環境が存在するものとする。この環境で、ドメインＢに属するサプリカント（Ｂ）が、ドメインＡのネットワークに参加したり、逆に、ドメインＡに属するサプリカント（Ａ）が、ドメインＢのネットワークに参加できるように環境を構築するには、第１の方法として、新たな一つのドメイン（ドメインＣ）に纏め直すか、あるいは、第２の方法として、それぞれのオーセンティケーションサーバが協調して、認証を請け負うように環境を構築する必要がある。ここで、「オーセンティケーションサーバの協調」とは、たとえば、ＲＡＤＩＵＳ　Ｐｒｏｘｙのような機能も含んでいる。

【００１２】

上記第１の方法については、新たなネットワーク環境を構築しなければならないことからコストがかかる。また、第２の方法は、ネットワークを構築する上では簡易であるが、かならずしも、すべてのオーセンティケーションサーバに協調できるような機能がついているわけではなく、システム構成上の不安定要因を含んでいる。

【００１３】

このように、従来では、各々異なるドメイン下にある各サプリカントが、それぞれのドメインのオーセンティケータを通してネットワークに参加できるシステムを構築しようとした際、種々の問題があった。

【００１４】

【非特許文献１】

認証サーバソフトウェア　株式会社アクセンス・テクノロジー　ｈｔｔｐ：／／ａｃｃｅｎｓｅ．ｃｏｍ／ｆｕｌｌｆｌｅｘ

【００１５】

【非特許文献２】

ＩＥＥＥ規格書８０２．１ｘ－２００１「ポート依存型ネットワークアクセス制御」（Ｐｏｒｔ－Ｂａｓｅｄ　Ｎｅｔｗｏｒｋ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）（２００１年６月１４日）

【００１６】

【発明が解決しようとする課題】

上述したように、従来では、複数の環境（たとえばドメイン）下にある各サプリカントが、それぞれの環境（ドメイン）のオーセンティケータを通してネットワークに参加できるシステムを構築しようとした際、種々の問題があった。

【００１７】

本発明は上記実情に鑑みなされたもので、ネットワーク環境を異にする各端末が、それぞれ相互のネットワーク環境下でアクセスできるシステムを構築する際に、高度のユーザ認証機構を経済的に有利な構成で容易に構築することのできるネットワークシステム、情報処理装置、中継器およびネットワークシステムの構

築方法を提供することを目的とする。

【００１８】

また、本発明は、ドメイン等のネットワーク環境の再構築や、オーセンティケーションサーバの協調をおこなうことなく、複数の環境下にあるサプリカントが、それぞれ相互の環境下でアクセスできるネットワークシステムを構築できる情報処理装置、および中継器を提供することを目的とする。

【００１９】

【課題を解決するための手段】

本発明は、ネットワーク接続に際して認証を必要とする端末からの認証要求に対して、その要求を受け付けた中継機能をもつ処理が、上記要求受付時の情報を用いて、適切な認証用サーバを選別することを特徴とする。

【００２０】

即ち、本発明は、ネットワーク接続を行う端末と、前記端末の接続要求に際して認証を行うサーバと、前記端末からの認証要求を受け付け、当該要求受付時の情報をもとに前記端末の認証を行うサーバを特定し、前記要求を行った端末を前記特定したサーバに接続する処理装置とを具備したネットワークシステムを特徴とする。

【００２１】

また、本発明は、ネットワーク接続を行う端末装置から認証要求を受け付ける手段と、前記受け付けた要求をもとに当該要求を行った端末装置のアクセス資格の有無を検証する装置を特定する手段と、前記要求を行った端末装置を前記特定した装置に接続する手段とを具備した情報処理装置を特徴とする。

【００２２】

また、本発明は、端末の接続要求に際して認証を行うサーバを具備したネットワークシステムに設けられる中継器に於いて、端末からの認証要求をもとに当該要求を行った端末の認証を行うサーバを特定する手段と、前記要求を行った端末を前記特定したサーバに接続する手段とを具備したことを特徴とする。

【００２３】

また、本発明は、ネットワーク接続を行う端末と、前記端末からの要求に従い

前記端末をネットワークに接続する中継装置と、前記端末の接続要求に際して認証を行うサーバとを具備したネットワークシステムの構築方法に於いて、前記中継装置に、前記端末からの認証要求を受け付け、当該要求受付時の情報をもとに前記端末の認証を行うサーバを特定する手段と、前記要求を行った端末を前記特定したサーバに接続する手段とを備えて、前記端末が自己の認証を行うサーバとは異なるネットワーク環境下に於いても自己の認証を行うサーバとの間で認証手続きを行うことができるようにしたことを特徴とする。

【００２４】

上記したような本発明の機能を備えることにより、ドメイン等のネットワーク環境を異にする各端末が、それぞれ相互のネットワーク環境下でアクセスできるシステムを構築する際に、高度のユーザ認証機構を経済的に有利な構成で容易に構築することができる。たとえば、ＩＥＥＥ　８０２．１Ｘの定義に従えば、サプリカントからの認証要求に対して、その要求を受け付けたオーセンティケータが、ネットワーク接続可能なドメイン等のネットワーク環境それぞれに置かれたオーセンティケーションサーバの中から、適切な（上記要求を出したサプリカントの認証を行う）オーセンティケーションサーバを選別することが可能となる。この機能により、複数のドメイン等のネットワーク環境下にあるサプリカントが、ドメインの再構築や、オーセンティケーションサーバの協調をおこなうことなく、ネットワーク接続を行う任意のドメイン等の環境下に於いて、そこに存在するのオーセンティケータを通して、ネットワークに参加することができる。即ち、サプリカントは自己の所属するドメイン等の環境だけでなく、他の環境下にあるオーセンティケータとのアクセスで、自己の認証を行うオーセンティケーションサーバに対して認証を要求でき、その環境下でネットワーク接続を行うことができる。

【００２５】

【発明の実施の形態】

以下、図面を参照して本発明の実施形態を説明する。

【００２６】

図１は本発明の実施形態に於けるシステムの構成を示すブロック図であり、こ

こでは、ドメインＡの各コンポーネント（２０Ａ，３０Ａ，４０Ａ）がＩＰ網１０を介してドメインＢの各コンポーネント（２０Ｂ，３０Ｂ，４０Ｂ）にネットワーク接続された例を示している。

【００２７】

ドメインＡには、オーセンティケーションサーバ（ Authentication Server）となるＲＡＤＩＵＳサーバ２０（Ａ）、およびオーセンティケータ（ Authenticator）となるアクセスポイント（ＡＰ）３０（Ａ）が設けられる。更に、サプリカント（Supplicant）となるステーション（ＳＴＡ）４０（Ａ）が設けられる。

【００２８】

ドメインＢには、オーセンティケーションサーバ（ Authentication Server）となるＲＡＤＩＵＳサーバ２０（Ｂ）、およびオーセンティケータ（ Authenticator）となるアクセスポイント（ＡＰ）３０（Ｂ）が設けられる。更に、サプリカント（Supplicant）となるステーション（ＳＴＡ）４０（Ｂ）が設けられる。尚、ここでは、説明を簡素にするため、各ドメインに於いて各コンポーネントをそれぞれ１台ずつ示している。また、上記各ドメインに設けられたステーション（ＳＴＡ）４０（Ａ），４０（Ｂ）は、それぞれ汎用のパーソナルコンピュータを用いて実現され、各アクセスポイント（ＡＰ）３０（Ａ），３０（Ｂ）と、ステーション（ＳＴＡ）４０（Ａ），４０（Ｂ）との間は、それぞれ無線ＬＡＮにより接続されるものとする。

【００２９】

上記各アクセスポイント（ＡＰ）３０（Ａ），３０（Ｂ）には、それぞれ図２に示すようなルールテーブル（ＲＴ）３１が設けられる。

【００３０】

このルールテーブル（ＲＴ）３１は、各ステーション（ＳＴＡ）４０（Ａ），４０（Ｂ）からの認証要求に対して、そのステーションの認証を行うＲＡＤＩＵＳサーバを特定する際に用いられるもので、図２に示すように、ネットワーク接続が可能な各ドメインに設けられたＲＡＤＩＵＳサーバ２０（Ａ），２０（Ｂ）の情報（ＲＡＤＩＵＳ情報）と、その各ＲＡＤＩＵＳサーバ２０（Ａ），２０（Ｂ）が所属するドメインを特定できる比較文字列（条件パターン）とが対応付け

て設定され登録されている。

【００３１】

上記ルールテーブル（ＲＴ）３１上の比較文字列（条件パターン）は、認証手続きの際にステーション（ＳＴＡ）４０（Ａ），４０（Ｂ）から送られてくる、ＥＡＰ－Ｒｅｓｐｏｎｓｅ／Ｉｄｅｎｔｉｔｙ（この実施形態ではサプリカント識別情報と称す）とのパターンマッチングの際に参照されるもので、その具体的なパターンマッチングについては図５を参照して後述する。

【００３２】

図３は上記ルールテーブル（ＲＴ）３１を用いたアクセスポイント（ＡＰ）３０（Ａ），３０（Ｂ）の処理手順を示すフローチャートであり、ステーション（ＳＴＡ）４０（Ａ／Ｂ）から認証要求を受け付けた際に実行される。

【００３３】

図４は本発明の動作概念を示したもので、ここではＩＥＥＥ　８０２．１Ｘの定義に従うコンポーネントを対象に、ドメインＡ，Ｂ間に於ける認証手続のルートを例に示している。

【００３４】

図５は、上記実施形態に於いて、上記各アクセスポイント（ＡＰ）３０（Ａ），３０（Ｂ）がステーション（ＳＴＡ）４０（Ａ／Ｂ）から認証要求を受け付けた際に実行される上記ルールテーブル（ＲＴ）３１を用いたパターンマッチングの動作を説明するためのサプリカント識別情報（ＥＡＰ－Response／Identity）の一例を示したもので、ここではドメイン名を含んだ形式の記載を例に示している。

【００３５】

図６は上記認証時の処理およびデータの流れを簡単に示したもので、ここではＩＥＥＥ　８０２．１Ｘの定義に従うコンポーネントを対象に示している。また、ここではオーセンティケーションサーバ（ Authentication Server）にＲＡＤＩＵＳサーバを使用しているが、これに限るものではない。

【００３６】

図中の（３）と（４）との間で、図３に示す、認証要求に従うＲＡＤＩＵＳサ

ーバ２０（Ａ／Ｂ）を特定する処理が実行される。

【００３７】

ここで、上記図１乃至図６を参照して本発明の実施形態に於ける動作を説明する。

【００３８】

本発明の実施形態を説明するに際して、認証要求時に於けるデータの流れを図６を参照して説明する。ここでは認証が成功した例を示している。

【００３９】

（１）ＥＡＰＯＬ－Ｓｔａｒｔ

サプリカント（Supplicant）がオーセンティケータ（ Authenticator）に認証の開始を要求する。

【００４０】

（２）ＥＡＰ－Ｒｅｑｕｅｓｔ／Ｉｄｅｎｔｉｔｙ

オーセンティケータ（ Authenticator）がサプリカント（Supplicant）にサプリカント識別情報（ＥＡＰ－Response／Identity）を要求する。

【００４１】

（３）ＥＡＰ－Ｒｅｓｐｏｎｓｅ／Ｉｄｅｎｔｉｔｙ

サプリカント（Supplicant）がオーセンティケータ（ Authenticator）にサプリカント識別情報（ＥＡＰ－Response／Identity）を返答する。

【００４２】

（４）Ａｃｃｅｓｓ　Ｒｅｑｕｅｓｔ

オーセンティケータ（ Authenticator）がオーセンティケーションサーバ（ Authentication Server）にサプリカント（Supplicant）の認証を要求する。上記（３）と（４）の間に於いて、図３に示す処理が行われる。

【００４３】

（５）Ａｃｃｅｓｓ　Ｃｈａｌｌｅｎｇｅ

オーセンティケーションサーバ（ Authentication Server）からオーセンティケータ（ Authenticator）に、認証のためのチャレンジが返される。

【００４４】

（６）ＥＡＰ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｐｒｏｃｅｓｓ

サプリカント（Supplicant）とオーセンティケーションサーバ（ Authentication Server）との間で認証処理が行われる。本来、細かいやりとりを行っているが、ここでは省略する。

【００４５】

（７）Ａｃｃｅｓｓ　Ａｃｃｅｐｔ

オーセンティケーションサーバ（ Authentication Server）がオーセンティケータ（ Authenticator）に、サプリカント（Supplicant）を認証した旨を通知する。認証に失敗した場合は、Ａｃｃｅｓｓ　Ｒｅｊｅｃｔが返る。

【００４６】

（８）ＥＡＰ－Ｓｕｃｃｅｓｓ

オーセンティケータ（ Authenticator）がサプリカント（Supplicant）に、認証が成功した旨を通知する。

【００４７】

ここで、本発明の基本的な動作概念を図４を参照して説明する。

【００４８】

ドメインＡに於いてサプリカント（Supplicant）のアクセスを行うオーセンティケータ（ Authenticator）Ａは、サプリカント（Supplicant）Ｂが（例えば無線ＬＡＮを介して）ポートに接続してきた際、サプリカント（Supplicant）Ｂの認証を行うオーセンティケーションサーバ（ Authentication Server）Ｂを選択して、認証処理を開始する。この際、オーセンティケータ（ Authenticator）Ａは、ポートに接続してきたサプリカント（Supplicant）が、どのドメインに属しているのか判別する必要がある。この判別の際に、サプリカント（Supplicant）から受けた、上記図６（３）に示されるサプリカント識別情報（ＥＡＰ－Response／Identity）を利用する。

【００４９】

このサプリカント識別情報（ＥＡＰ－Response／Identity）には、サプリカント（Supplicant）の識別名が記載されている。この記載内容については、特に規定されていないが、たとえば、図５に示すようなドメイン名を含んだ形式で記載

される。

【００５０】

図６（３）に於いて、サプリカント識別情報（ＥＡＰ－Response／Identity）が、サプリカント（Supplicant）から送信されるので、オーセンティケータ（Authenticator）は、そのサプリカント識別情報（ＥＡＰ－Response／Identity）から、そのサプリカント（Supplicant）が属しているドメインを判別し、そのドメインに属している適切なオーセンティケーションサーバ（Authentication Server）に対して上記図６（４）以降の通信を開始する。

【００５１】

次に、図１に示すネットワークシステムに於ける認証処理について、図１乃至図３を参照して説明する。

【００５２】

図１に於いて、ＲＡＤＩＵＳサーバ２０（Ａ）は、ドメインＡに属する各ステーション（ＳＴＡ）４０（Ａ）の認証を行う。ＲＡＤＩＵＳサーバ２０（Ｂ）はドメインＢに属する各ステーション（ＳＴＡ）４０（Ｂ）の認証を行う。

【００５３】

アクセスポイント（ＡＰ）３０（Ａ）は、ドメインＡに属するステーション（ＳＴＡ）４０（Ａ）のアクセスを制御する。アクセスポイント（ＡＰ）３０（Ｂ）は、ドメインＢに属するステーション（ＳＴＡ）４０（Ｂ）のアクセスを制御する。

【００５４】

ステーション（ＳＴＡ）４０（Ａ），４０（Ｂ）は、上記各アクセスポイント（ＡＰ）３０（Ａ），３０（Ｂ）との間で、例えば無線ＬＡＮを介して接続される。尚、図１では、ステーションＳＴＡ）４０（Ｂ）が、例えば携帯型のパーソナルコンピュータを用いて構成され、本来、所属するドメインＢのアクセスポイント（ＡＰ）３０（Ｂ）から切り離されて、ドメインＡのアクセスポイント（ＡＰ）３０（Ａ）に接続要求を行う場合を例示している。

【００５５】

この際、アクセスポイント（ＡＰ）３０（Ａ）は、ステーション（ＳＴＡ）４０（Ｂ）から接続要求に際して、認証要求（図６（１）に示すＥＡＰＯＬ－Ｓｔａｒｔ；認証の開始要求）を受けることにより、上記した図６に示す認証のためのデータ授受が開始される。この図６に示す（３）と（４）の間に於いて、図３に示す、認証要求に従うＲＡＤＩＵＳサーバ２０（Ａ／Ｂ）を特定する処理が実行される。

【００５６】

この処理は、図２に示すルールテーブル（ＲＴ）３１を参照して行われる。

【００５７】

アクセスポイント（ＡＰ）３０（Ａ）は、ステーション（ＳＴＡ）４０（Ｂ）から上記認証の開始要求を受けると（図６（１）参照）、ステーション（ＳＴＡ）４０（Ｂ）にサプリカント識別情報（ＥＡＰ－Response／Identity）を要求する（図６（２）参照）。

【００５８】

この要求に従い、ステーション（ＳＴＡ）４０（Ｂ）からサプリカント識別情報（ＥＡＰ－Response／Identity）を取得すると、そのサプリカント識別情報（ＥＡＰ－Response／Identity）に含まれる図５に示すような識別名の一部（例えばドメイン名）を用いて、図２に示すルールテーブル（ＲＴ）３１とのパターンマッチングにより、ステーション（ＳＴＡ）４０（Ｂ）の認証を行うＲＡＤＩＵＳサーバ２０（Ａ／Ｂ）を検索する。即ち、認証要求を出したステーション（ＳＴＡ）４０（Ｂ）と同じドメイン名若しくはそれに類する文字列構造をもつＲＡＤＩＵＳ情報を検索する（図３ステップＳ３１，Ｓ３２）。

【００５９】

ここで、ステーション（ＳＴＡ）４０（Ｂ）と同じドメイン名若しくはそれに類する文字列構造をもつＲＡＤＩＵＳ情報が存在（パターンマッチ）すると、ルールテーブル（ＲＴ）３１のパターンマッチした個所に記述されているＩＰアドレス、ポート番号等から認証要求先のＲＡＤＩＵＳサーバ２０（Ｂ）を決定し（図３ステップＳ３３）、決定したＲＡＤＩＵＳサーバ２０（Ｂ）に図６（４）に示すＡｃｃｅｓｓ　Ｒｅｑｕｅｓｔを送付して認証を要求する。

【００６０】

このような処理により、ドメインの再構築や、オーセンティケーションサーバ同士が協調して動作しなくても、ネットワーク環境を異にする各端末（ステーション）が、それぞれ相互のネットワーク環境下でアクセスできる。

【００６１】

尚、本発明は、ＩＥＥＥ　８０２．１Ｘに限らず、ＥＡＰ（Extensible Authentication Protocol）による認証プロトコルを採用し、かつ、端末と認証サーバの間に立って、中継をおこなうようなすべてのシステムに適用できる。たとえば、ＲＡＳ（Remote Access Server）にも適用可能である。

【００６２】

【発明の効果】

以上詳記したように、本発明によれば、ネットワーク環境を異にする各端末が、それぞれ相互のネットワーク環境下でアクセスできるシステムを構築する際に、高度のユーザ認証機構を経済的に有利な構成で容易に構築することができる。

【図面の簡単な説明】

【図１】

本発明の第１実施形態に於けるシステムの構成を示すブロック図。

【図２】

上記実施形態に於けるルールテーブル（ＲＴ）の構成例を示す図。

【図３】

上記実施形態に於けるルールテーブル（ＲＴ）を用いたアクセスポイントの処理手順を示すフローチャート。

【図４】

本発明の動作概念を示す図。

【図５】

上記実施形態に於けるルールテーブル（ＲＴ）を用いたパターンマッチングの動作を説明するためのサプリカント識別情報（ＥＡＰ－Ｒｅｓｐｏｎｓｅ／Ｉｄｅｎｔｉｔｙ）の一例を示す図。

【図６】

上記実施形態に於ける認証時の処理の流れを示す図。

【図７】

本発明で対象とするネットワーク環境の基本的な構成例を示す図。

【符号の説明】

１０…ＩＰ網

２０（Ａ），３０（Ｂ）…ＲＡＤＩＵＳサーバ

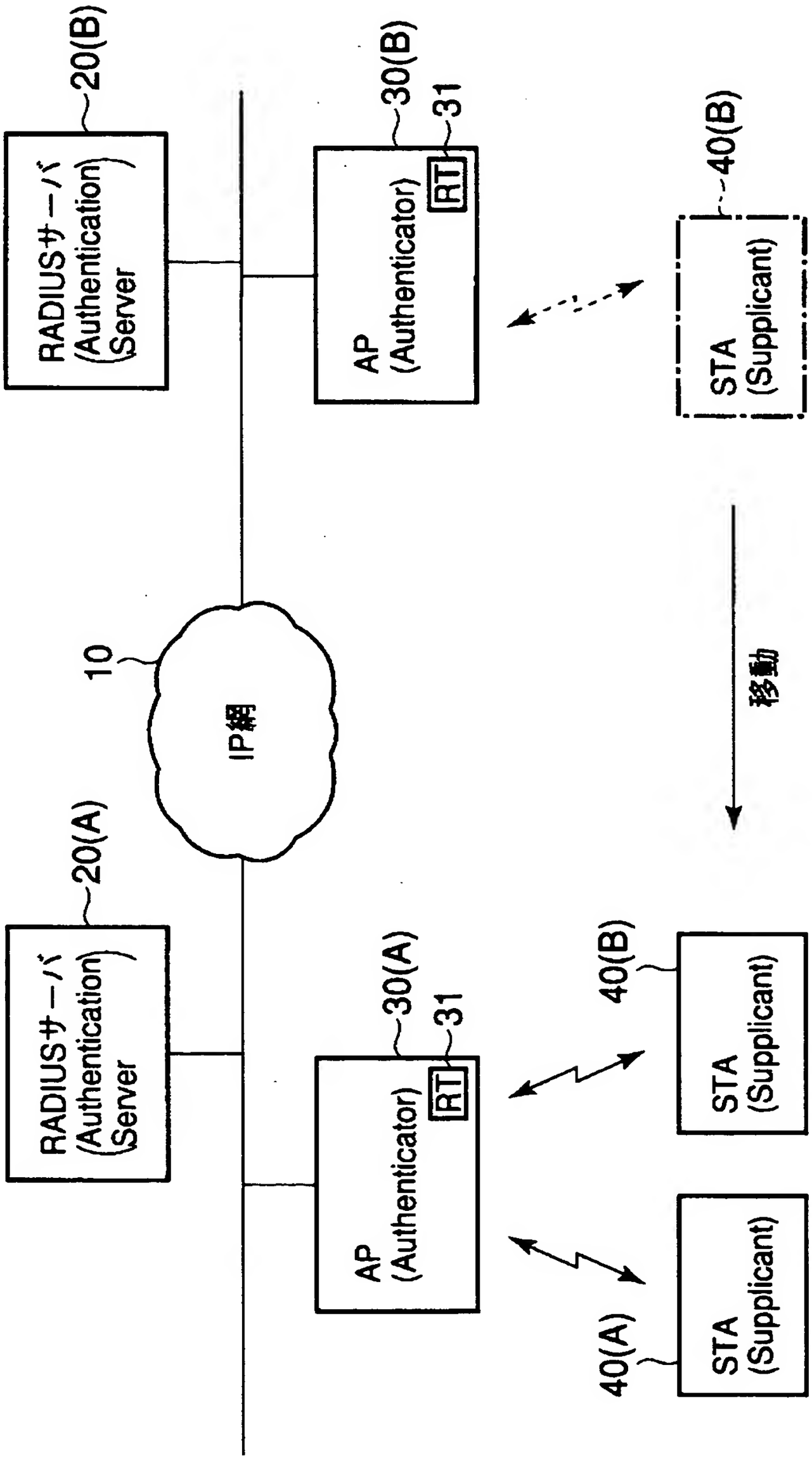
３０（Ａ），３０（Ｂ）…アクセスポイント（ＡＰ）

３１…ルールテーブル（ＲＴ）

４０（Ａ），４０（Ｂ）…ステーション（ＳＴＡ）

【書類名】　　図面

【図１】

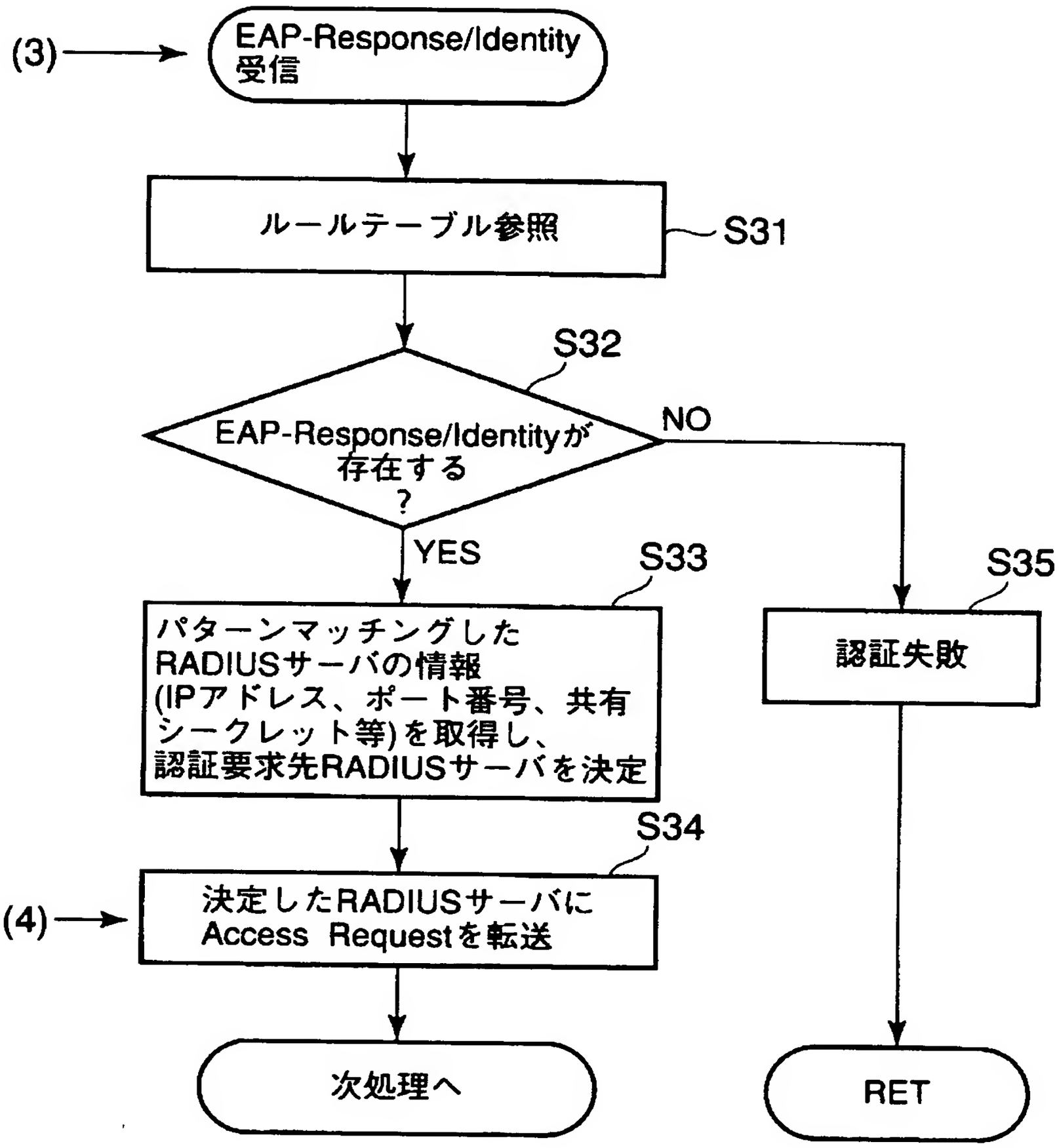

RADIUSサーバ
(Authentication)
Server
20(B)
AP
(Authenticator)
RT
30(B)
31
40(B)
STA
(Supplicant)
移動
IP網
10
20(A)
30(A)
40(A)

【図２】

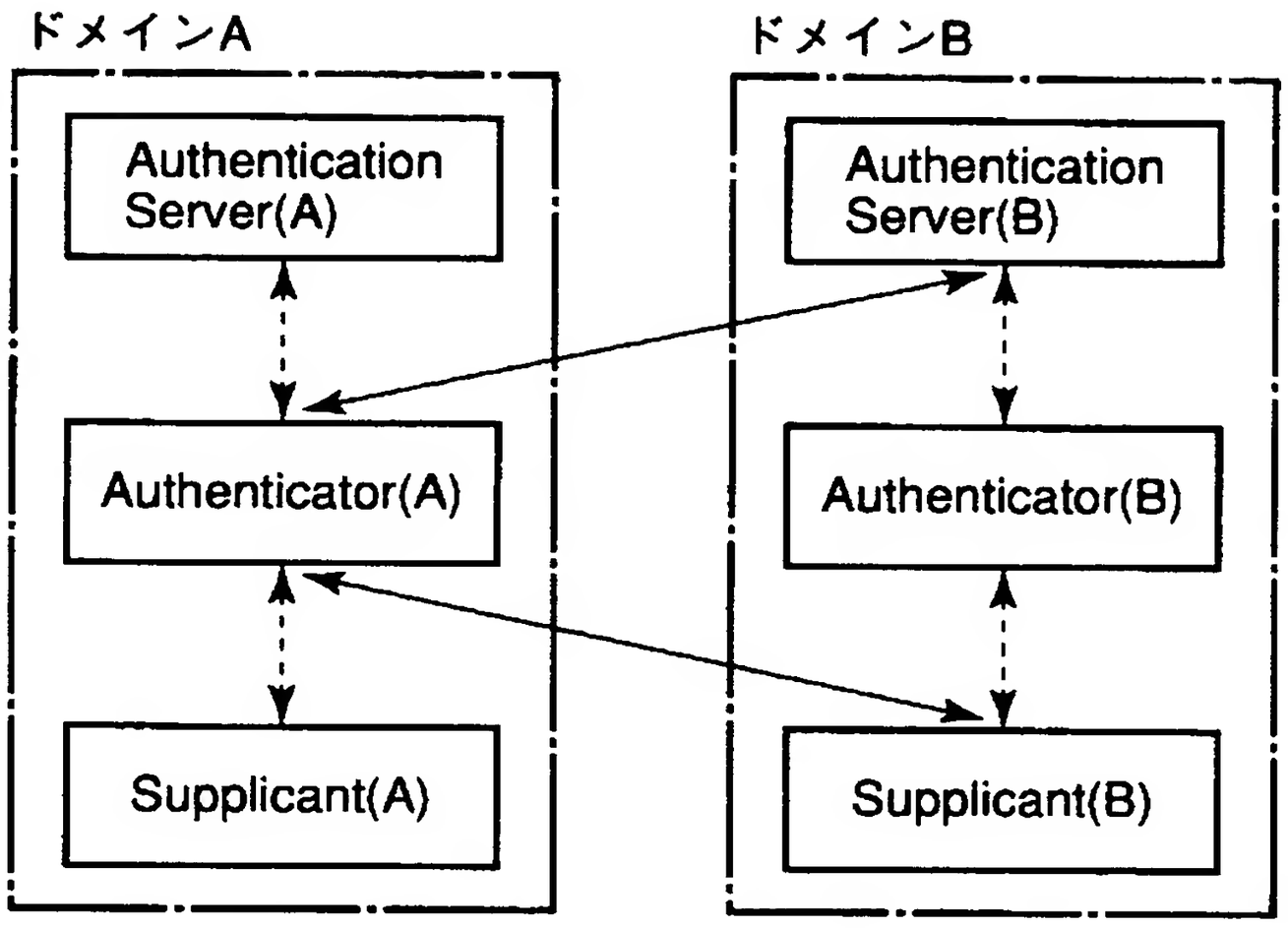
ルールテーブル(RT)　31

| EAP-Response/Identity<br>比較文字列(条件パターン) | RADIUS情報<br>(IPアドレス、ポート番号、<br>共有シークレット等) |
|---|---|
| DOMAIN-B¥＊ | RADIUS-B |
| ＊@domain-a.・・・・.co.jp | RADIUS-A |
| ⋮ | ⋮ |

【図３】


(3)
EAP-Response/Identity
受信
ルールテーブル参照
S31
S32
EAP-Response/Identityが
存在する
?
NO
YES
S33
パターンマッチングした
RADIUSサーバの情報
(IPアドレス、ポート番号、共有
シークレット等)を取得し、
認証要求先RADIUSサーバを決定
S34
(4)
決定したRADIUSサーバに
Access Requestを転送
次処理へ
S35
認証失敗
RET

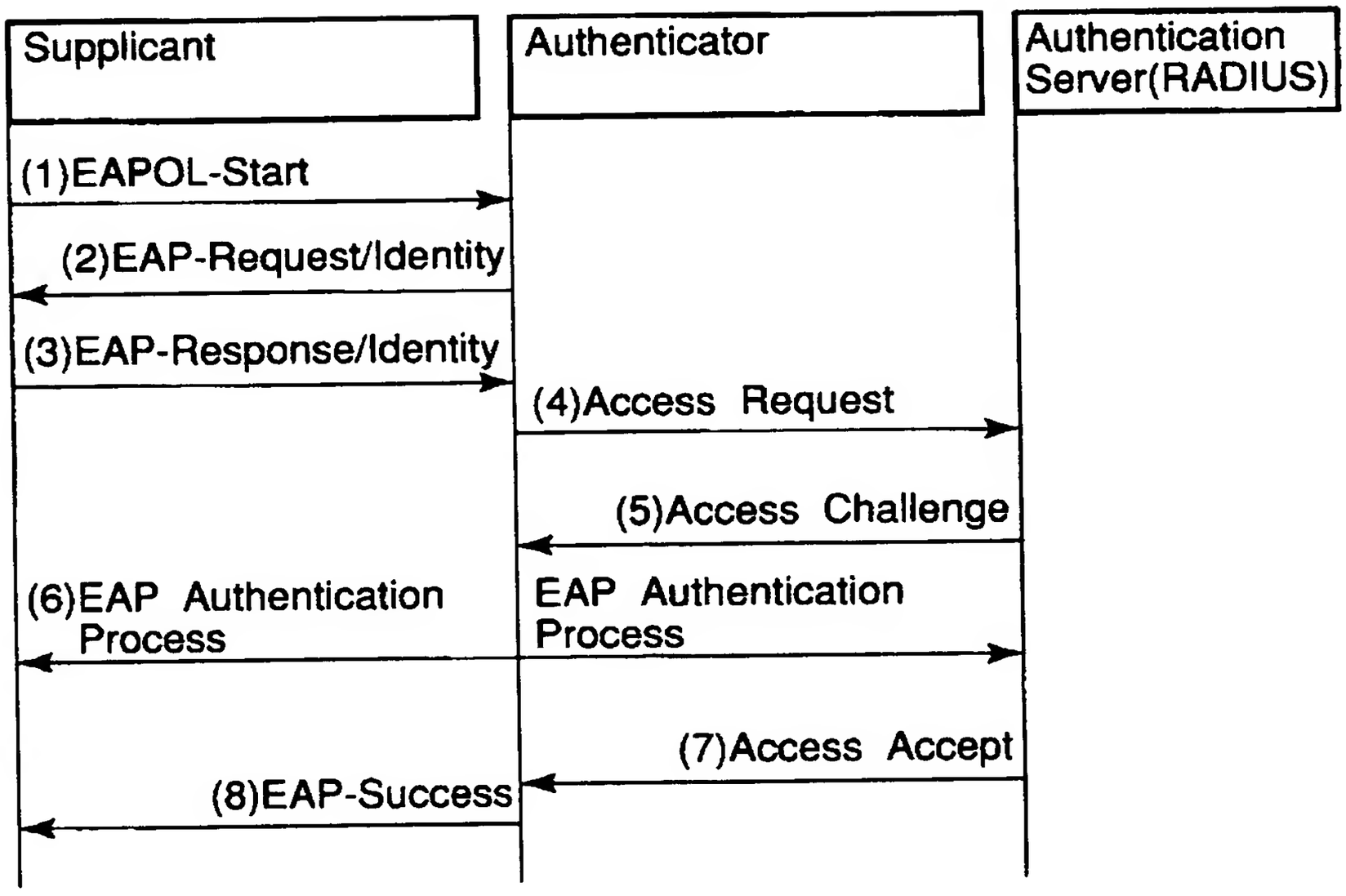
【図４】



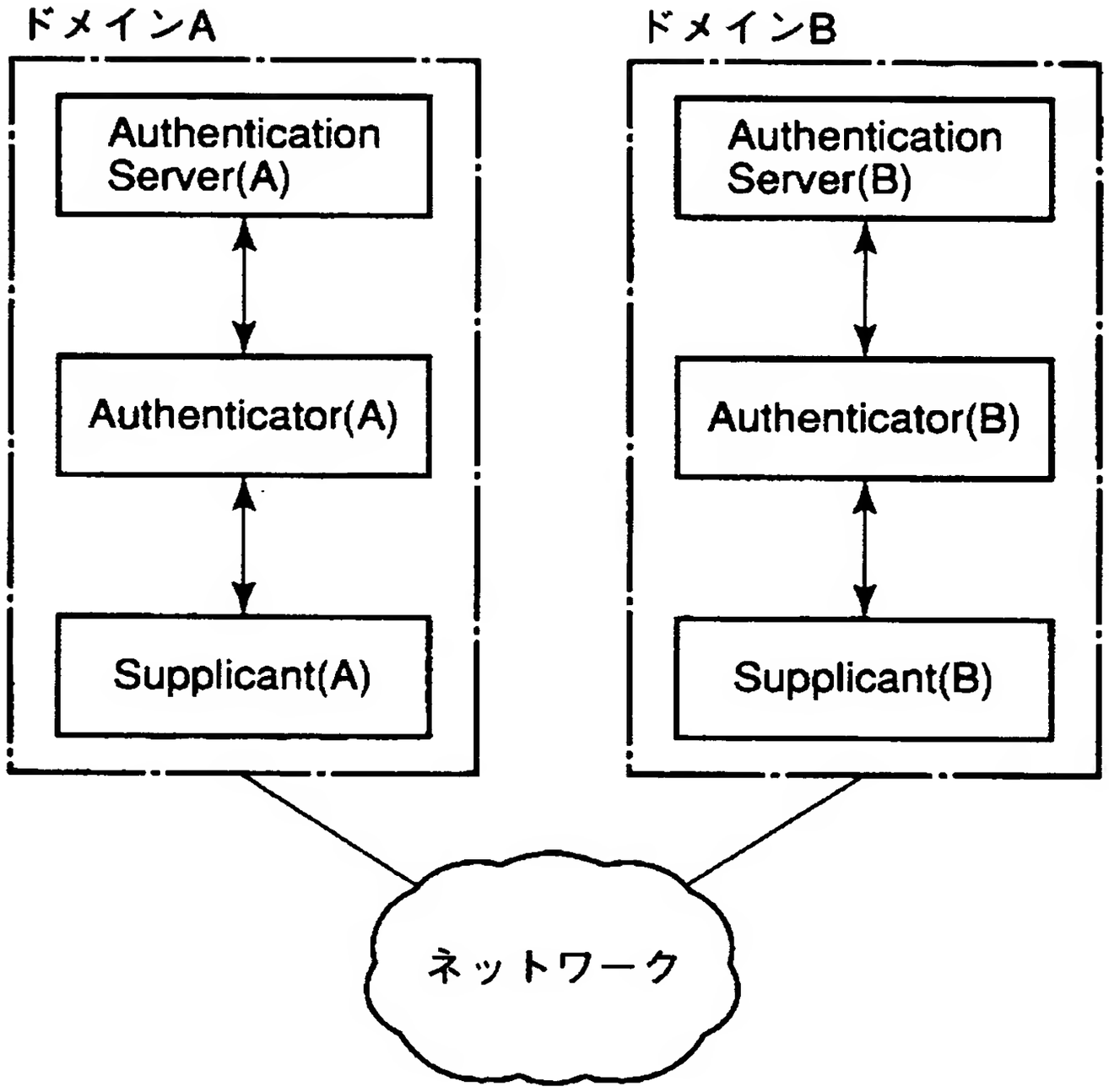

【図５】

| | |
|---|---|
| NETBIOS ドメイン名を使用した表現 | ＜ドメイン名＞￥＜ユーザ名＞の形式で記載される<br>例：DOMAIN-A¥user01 |
| DNS ドメイン名を使用した表現 | ＜ユーザ名＞@＜ドメイン＞の形式で記載される<br>例：user01@domain-a.tos×××.co.jp |

【図６】


Supplicant
Authenticator
Authentication Server(RADIUS)
(1)EAPOL-Start
(2)EAP-Request/Identity
(3)EAP-Response/Identity
(4)Access Request
(5)Access Challenge
(6)EAP Authentication Process
EAP Authentication Process
(7)Access Accept
(8)EAP-Success

【図７】


ドメインA
ドメインB
Authentication Server(A)
Authenticator(A)
Supplicant(A)
Authentication Server(B)
Authenticator(B)
Supplicant(B)
ネットワーク

【書類名】　　要約書

【要約】

【課題】本発明は、ドメイン等のネットワーク環境の再構築や、オーセンティケーションサーバの協調をおこなうことなく、複数の環境下にあるサプリカントが、それぞれ相互の環境下でアクセスできるネットワークシステム、中継装置、およびその構築方法を提供することを課題とする。

【解決手段】アクセスポイント（ＡＰ）３０（Ａ）は、ステーション（ＳＴＡ）４０（Ｂ）から認証の開始要求を受けると、ステーション（ＳＴＡ）４０（Ｂ）からサプリカント識別情報（ＥＡＰ－Response／Identity）を取得して、ルールテーブル（ＲＴ）３１とのパターンマッチングにより、アクセスポイント（ＡＰ）３０（Ｂ）の認証を行うＲＡＤＩＵＳサーバ２０（Ａ／Ｂ）を検索する。

【選択図】　　図１

# 出　願　人　履　歴　情　報

識別番号　　〔０００００３０７８〕

１．変更年月日　　２００１年　７月　２日
　［変更理由］　　住所変更
　　住　所　　東京都港区芝浦一丁目１番１号
　　氏　名　　株式会社東芝